Delgado COMMUNITY COLLEGE

POLICY No. IT-001

INTERNAL/DEPARTMENTAL POLICY AND PROCEDURE

TITLE: **Gramm-Leach-Bliley Act (GLBA) Security Program**

EFFECTIVE DATE: **December 9, 2024**

CANCELLATION: none

DIVISION: INFORMATION TECHNOLOGY

CATEGORY: Information Technology (IT)

RESPONSIBLE DEPARTMENT: Office of Information Technology

PROCEDURES & SPECIFIC INFORMATION

1. **Purpose**

The purpose of this document is to summarize Delgado Community College's comprehensive written information security program (the "Program") mandated by the Federal Trade Commission's Safeguards Rule and the Gramm – Leach – Bliley Act ("GLBA").

In particular, this document describes the Program elements pursuant to which the College intends to (i) ensure the security and confidentiality of covered records, (ii) protect against any anticipated threats or hazards to the security of such records, and (iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers. The Program incorporates by reference the College's policies and procedures enumerated in this document and is in addition to any College policies and procedures that may be required pursuant to other federal and state laws and regulations, including, without limitation, FERPA.

2. **Scope and Authority of Program**

The Program applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the College, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the College or its affiliates. For these purposes, the term nonpublic financial information shall mean any information (i) a student or other third party provides in order to obtain a financial service from the College, (ii) about a student or other third party resulting from any transaction with the College involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person. *This scope does not cover any data maintained by the Louisiana Community and Technical College System (LCTCS) office or associated information systems.*

3. **Designation of Representatives**

The College's Chief Information Officer is designated as the Program Officer who shall be responsible for coordinating and overseeing the Program. The Program Officer may designate other representatives of the College to oversee and coordinate particular elements of the Program. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the Program Officer or designee(s).

4. **Elements of the Program**

A. **Risk Identification and Assessment.** The College intends, as part of the Program, to undertake to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. In implementing the Program, the Program Officer will establish procedures for identifying and assessing such risks in each relevant area of the College's operations, including:

(1) *Risk Assessment*

The College routinely undertakes actions such as the following to assess risk and ensure security prevention.

- Adopting Center for Internet Security (CIS) Critical Security Controls [a global IT-prioritized set of actions (framework/best practices) to protect an organization and data from cyberattacks]
- Utilizing Wireless Internet Service Providers (WISP) [ensures all providers utilize tools to mitigate cybersecurity risks on a wireless network (i.e., required strong passwords, encryption standards/ protocols, regular firmware updates, network segmentation, firewalls, access controls, etc.]
- Participating in the LCTCS Cyber Security Awareness Program and Training Portal
- Developing, Accepting, and Implementing the College's Information Security Policy
- Practicing Payment Card Industry (PCI) Security Standards (ensures third-party applications used by the College for finance matters follow industry payment standards)
- Performing Cyber Hygiene Assessments
- Utilizing Qualys Security Scans
- Performing Third Party Security Assessments
- Performing Annual IT Risk Assessment Check
- Employee training and management. The Program Officer will coordinate with appropriate representatives at the College and other affected units to provide training and management related to procedures and practices for accessing and using student records, including financial aid information. This evaluation will include assessing the effectiveness of the College's current policies and procedures in this area, including but not limited to Delgado's Information Security and Student Records policies.

(2) *Information Systems and Information Processing and Disposal*

The Program Officer will coordinate with appropriate representatives at the College and other affected units to assess the risks to nonpublic financial information associated with the College's information systems, including network and software design, information processing, and the storage, transmission and disposal of nonpublic financial information. This evaluation will include assessing the College's current policies and procedures relating to acceptable use of the College's network and network security, document retention and destruction, including but not limited to the Delgado's Information Security, Record Retention, Transfer and Disposal of Electronic Media and Devices, and Student Records policies. The Program Officer will also coordinate with the College's departments to assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

(3) *Detecting, Preventing and Responding to Attacks*

The Program Officer will reference the Delgado Incident Response Plan outlined in the College's Information Security Policy, where appropriate, or coordinate with appropriate representatives at the College and other affected units to evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. In this regard, the Program Officer may elect to delegate to a representative from departments the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the College.

B. **Designing and Implementing Safeguards**.

The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The Program Officer will regularly implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

C. **Overseeing Service Providers**

The Program Officer shall coordinate with those responsible for the third-party service procurement activities among the appropriate representatives at the College departments and other affected units to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they will have access. In addition, the Program Officer will work with the College's relevant department providers to implement and maintain appropriate safeguards.

D. **Adjustments to Program**

The Program Officer will periodically evaluate and adjust the Program based on the risk identification and assessment activities, test results, data governance requirements, and other major changes to operations or business, or other material changes or circumstances that may impact the Program.

Review/Approval Process:

Ad Hoc Committee on GLBA Security Program Policy 12/9/24
Chief Information Officer Approval 12/9/24